IN THE CLAIMS:

1-16. (Cancelled)

17. (Currently Amended) A file decryption apparatus that decrypts a ciphertext, the file decryption apparatus comprising:

a memory unit for storing an encrypted key, a ciphertext, and an encrypted file key, the encrypted key being generated by encrypting original key information stored in a portable key storage medium using a first password inputted by a user , the encrypted file key being generated by encrypting [[a]] an original file key using the original key information, and the ciphertext being generated by encrypting a plaintext using the original file key;

a switch unit

(a) including a first key obtaining unit operable to receive an input of a second password from the user and decrypt the encrypted key stored in the memory unit using the received second password to generate decrypted key information, and a second key obtaining unit operable to read the original key information from the key storage medium loaded in the file decryption apparatus, and

(b) is operable to obtain either the original key information or the decrypted key information by one of the first key obtaining unit and the second key obtaining unit; and

a decryption unit operable to decrypt the encrypted file key using ~~the obtained key information~~ either the obtained original key information or the obtained decrypted key information to generate a decrypted file key, and decrypt the ciphertext using the decrypted file key to generate a decrypted text.

18-56. (Cancelled)

57. (Previously Presented) The file decryption apparatus of Claim 17, wherein

the memory unit further stores, in association with the encrypted key, a user identifier that identifies a user, and

the first key obtaining unit further receives an input of the user identifier from the user and decrypts the encrypted key that is associated with the user identifier.

58. (Currently Amended) The file decryption apparatus of Claim 17, wherein

the memory unit further stores, in association with the encrypted key, authentication information generated based on the original key information, and

the first key obtaining unit checks, using the authentication information, whether the encrypted key has been altered or not, when the encrypted key that is associated with the authentication information is decrypted.

59. (Previously Presented) The file decryption apparatus of Claim 17, wherein

the memory unit is a portable storage medium, and

the first key obtaining unit decrypts the encrypted key that has been written to the memory unit that is the portable storage medium.

60. (Previously Presented) The file decryption apparatus of Claim 17, wherein

the memory unit further stores the encrypted key in association with the ciphertext and the encrypted file key, and

the first key obtaining unit decrypts the encrypted key that is associated with the ciphertext and the encrypted file key.

61. (Previously Presented) The file decryption apparatus of Claim 17, wherein

the memory unit further stores, in association with the ciphertext, authentication information generated based on the ciphertext, and

the decryption unit checks, using the authentication information, whether the ciphertext has been altered or not, when the ciphertext that is associated with the authentication information is decrypted.

62. (Currently Amended) A file management apparatus that encrypts a plaintext to generate a ciphertext, stores the ciphertext, and decrypts the ciphertext, the file management apparatus comprising:

a memory unit;

a registration unit operable to receive an input of a first password from a user, generating an encrypted key by encrypting original key information, which is stored in a portable key storage medium, using the received first password, and writing the generated encrypted key to the memory unit;

an encryption unit operable to generate a ciphertext by encrypting a plaintext using [[a]] an original file key, generate an encrypted file key by encrypting the original file key using the key information stored in the key storage medium, and write the generated ciphertext and encrypted file key to the memory unit in association with each other;

a switch unit

(a) including a first key obtaining unit operable to receive an input of [[the]] a second password from the user and decrypt the encrypted key in the memory unit using the received second password to generate decrypted key information, and a second key obtaining unit operable to read the key information from the key storage medium loaded in the file management apparatus, and

(b) is operable to obtain either the original key information or the decrypted key information by one of the first key obtaining unit and the second key obtaining unit; and

a decryption unit operable to decrypt the encrypted file key using ~~the obtained key information~~ either the obtained original key information or the obtained decrypted key information to generate a decrypted file key, and decrypt the ciphertext using the decrypted file key to generate a decrypted text.

63. (Currently Amended) The file management apparatus of Claim 62,

wherein the registration unit further receives an input of a first user identifier that identifies a user, and writes the first user identifier in association with the encrypted key, to the memory unit, and

the first key obtaining unit further receives an input of [[the]] a second user identifier and decrypts the encrypted key that is associated with the received second user identifier.

64. (Currently Amended) The file management apparatus of Claim 62,

wherein the registration unit further writes

authentication information, which is generated based on the original key information, to the memory unit in association with the encrypted key,

the first key obtaining unit further checks, using the authentication information, whether the encrypted key has been altered or not, when the encrypted key that is associated with the authentication information is decrypted.

65. (Previously Presented) The file management apparatus of Claim 62,

wherein the encryption unit further writes authentication information, which is generated based on the ciphertext, to the memory unit in association with the ciphertext,

the decryption unit further checks, using the authentication information, whether the ciphertext has been altered or not, when the ciphertext that is associated with the authentication information is decrypted.

66. (Previously Presented) The file management apparatus of Claim 62,

wherein the memory unit is a portable storage medium, the registration unit writes the encrypted key to the memory unit being a portable storage medium, and

the first key obtaining unit decrypts the encrypted key in the memory unit being a portable storage medium.

67. (Previously Presented) The file management apparatus of Claim 62 further comprising

a deletion unit operable to delete the encrypted key that has been written to the memory unit.

68. (Currently Amended) The file management apparatus of Claim 62 further comprising

a deletion unit operable to delete the encrypted key that has been written to the memory unit,

wherein the registration unit further receives an input of a new password from the user, encrypts the original key information, which is stored in the key storage medium, using the new password to generate a new encrypted key, and writes the generated new encrypted key to the memory unit.

69. (Currently Amended) The file management apparatus of Claim 62,

wherein the key storage medium stores new key information, instead of the original key information,

the registration unit receives [[the]] an input of [[the]] a third password from a user and decrypts the encrypted key using the received third password to generate old key information,

the encryption unit includes a decryption sub-unit, ~~decrypts~~ causes the decryption sub-unit to decrypt the encrypted file key using the old key information to generate a generative file key, encrypts the generative file key using the new key information, which is stored in the key storage medium, to generate a new encrypted file key, and writes the new encrypted file key over the encrypted file key in the memory unit, and

the registration unit encrypts the new key *information* using the third password to generate a new encrypted key and writes the new encrypted key over the encrypted key in the memory unit.

70. (Currently Amended) The file management apparatus of Claim 69,

wherein the registration unit further receives an input of a user identifier that identifies a user,

the encryption unit further writes the user identifier in association with the ciphertext and the encrypted file key, to the memory unit, and the encryption unit retrieves the encrypted file key that is associated with the user identifier in the memory unit and generates [[a]] the generative file key from the retrieved encrypted file key.

71. (Currently Amended) The file management apparatus of Claim 69,

wherein the encryption unit further writes encryption information in association with the ciphertext and the encrypted file key, to the memory unit, the encryption information indicating that the plaintext has been encrypted, and

the encryption unit retrieves the encrypted file key that is associated with the encryption information in the memory unit, and generates [[a]] the generative file key from the retrieved encrypted file key.

72. (Currently Amended) The file management apparatus of Claim 69,

wherein the registration unit further receives an input of a user identifier that identifies a user,

the encryption unit further writes the user identifier in association with a file identifier that identifies the ciphertext and the encrypted file key, as a unified file, to the memory unit, and

the encryption unit extracts the file identifier that is associated with the user identifier from the unified file, specifies the encrypted file key identified by the extracted file identifier, and generates [[a]] the generative file key from the specified encrypted file key.

73. (Currently Amended) The file management apparatus of Claim 69,

wherein the encryption unit further writes encryption information in association with a file identifier that identifies the ciphertext and the encrypted file key, as a unified file, to the memory unit, the encryption information indicating that the plaintext has been encrypted, and

the encryption unit extracts the file identifier that is associated with the encryption information from the unified file specifies the encrypted file key identified by the extracted file identifier, and generates [[a]] the generative file key from the specified encrypted file key.

74. (Previously Presented) The file management apparatus of Claim 62,

wherein the encryption unit further writes the encrypted key in association with the ciphertext and the encrypted file key, to the memory unit, and

the first key obtaining unit decrypts the encrypted key that is associated with the ciphertext and the encrypted file key.

75. (Previously Presented) The file management apparatus of Claim 74,

wherein the encryption unit further receives an input of an indication, the indication showing whether the encrypted key and the ciphertext are to be written in association with each other to the memory unit, and writes, when the indication shows that the encrypted key and the ciphertext are to be written in association with each other, the encrypted key in association with the ciphertext, to the memory unit.

76. (Cancelled)